Social engineering and social media[1]

Bányász Péter[2]

Absztrakt:
A kibertérből érkező fenyegetések száma napjainkra folyamatosan növekszik, ami az infokommunikációs technológiák további várható növekedésével csak fokozódni fog. A támadások különböző motivációból fakadhatnak, állhatnak mögöttük hacktivisták, kiberbűnözők, terroristák, állami szervezetek, akik kémkedésre vagy hadviselésre használják a kiberteret. A lassan, mindent átszövő infokommunikációs hálózatok védelme ebből következően létfontosságú. Legyen azonban bármilyen fejlett egy rendszer fizikai és/vagy logikai védelme, a humán tényező mindig is kockázatot fog jelenteni. A social engineering annak a művészete, hogyan férhetnek hozzá a támadók egy védett rendszerhez az emberi tulajdonságok kihasználásával. Jelen tanulmány azokat a social engineering technikákat mutatja be, amelyek a közösségi oldalakon keresztül végezhetnek.

Kulcsszavak: közösségi média, social engineering, kiberbűnözés, kiberkémkedés, kiberhadviselés

Abstract:
The number of the threats,- which come from the cyber space- are increasing. These threats will increase more because of development of the infocommunication technologies. The motivation sources of these attacks are different. Hacktivist, cybercriminals, terrorists, public organizations, who use the cyberspace for spying or warfare. So the protection of the infocommunication network-which slowly pervade everything- is indispensable. However a system's physicaly and logical protection could be well developed, the human factor will be always a risk. The social engineering is an art, how attackers can hack a protected system by humanity. This paper presents those social engineering techniques which can be used on the social media sites. The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled „Public Service Development Establishing Good Governance" in the Ludovika Workshop.

Keywords: social media, social engineering, cyber crime, cyber espionage, cyber warfare

[1] A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés" elnevezésű kiemelt projekt keretében működtetett Ludovika Kiemelt Kutatóműhely keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

[2] Nemzeti Közszolgálati Egyetem Államtudományi és Közigazgatási Kar Elektronikus Közszolgálati Intézet, tanársegéd, ORCID: 0000-0002-7308-9304, elérhetőség: banyasz.peter@uni-nke.hu

Bevezetés

A Nemzetbiztonsági Szemle 2017. évi 4. számában jelent meg egy tanulmányom Kiberbűnözés és közösségi média címen,[3] amelyben egy alfejezet a social engineering támadásokkal is foglalkozott. A téma bősége okán azonban részletes ismertetésére csupán érintőlegesen nyílt mód. Jelen munkámban kísérletet teszek a problémakör szélesebb vizsgálatára, ugyanis megítélésem szerint a kibertámadások egy különösen jelentős fajtáját jelenti a social engineering, aminek vélelmezhetően a jövőben a száma növekedni, kifinomultsága erősödni fog.

Főbb fogalmak

Az említett tanulmányban megkülönböztettem a kiberfenyegetéseket motivációk szerint. „A kiberbűnözés (…) az informatikai eszközök segítségével olyan illegális cselekmények elkövetése, amely a támadóknak anyagi haszonnal kecsegtet. A második nagy csoport a hacktivizmus és kiberterrorizmus, amelyek bár fogalmilag eltérő tevékenységet jelölnek, azonban bizonyos közös vonzat kimutatható közöttük, mindkettő esetében kisebb, decentralizált csoportok működéséről beszélhetünk, amelyeknek célja a médiafigyelem elnyerése, hogy ezáltal hirdessék ideológiai céljaikat. A harmadik kategória a kiberkémkedés, amelyet az információs rendszerekben tárolt adatok megszerzésért végeznek állami és nem állami szereplők. Végül pedig negyedikként a kiberhadviselést kell említenünk, amely tevékenység az államok közti konfliktusokban jelenik meg, segítségével a szembenálló felek informatikai eszközöket alkalmaznak akár a konvencionális hadviselés támogatására, akár önálló tevékenység folytatására.”[4]

Legyen bármilyen motivációja a támadóknak, a social engineering, mint támadás típus mindegyikük eszköztárában szerepel. Ennek okául az a felismerés szolgál, hogy legyen egy rendszer bármennyire erős fizikai és/vagy logikai védelemmel5 ellátva, a gyenge pontját, amelyen keresztül sikeres támadást hajthatnak végre, igen nagy valószínűséggel a humán tényezőn keresztül érik el.

---

[3] *Bányász Péter: Kiberbűnözés és közösségi média, In. Nemzetbiztonsági Szemle, 2017/4., pp. 55-74., 2017.*

[4] *I.m. Bányász 2017, p. 56.*

[5] *A 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról értelmező rendelkezései alapján fizikai védelem: a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem; logikai védelem: az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem.*

Kevin D. Mitnick[6] megfogalmazásában „A social engineering a befolyásolás és rábeszélés eszközével megtéveszti az embereket, manipulálja vagy meggyőzi őket, hogy a social engineer tényleg az, akinek mondja magát. Ennek eredményeként a social engineer – technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni.”[7] A social engineering tehát egy olyan támadásforma, amelynek során az emberi tényező kihasználható aspektusaira épít, olyan technikák és módszerek összessége, amely az emberek befolyásolásával, adott esetben zsarolásával, megtévesztésével fér hozzá bizalmas információkhoz, rendszerekhez.[8]

Az ember jelenleg még mindig megkerülhetetlen a munkavégzésben. Hiába vált ki a robotizáció számos munkafolyamatot, még mindig az ember vezérli a különböző hardver és szoftver eszközöket, az ember fér hozzá rendszerekhez, azon keresztül különböző adatokhoz.[9] Az egyes emberek azonban rendkívül eltérő személyiséggel, különböző pszichológiai jellemvonásokkal, komplexusokkal, félelmekkel bírnak. Megkülönböztethetünk azonban bizonyos tulajdonságokat, amiket a támadók kijátszhatnak.[10] Ezek közé tartozik többek között:

- a segítségnyújtás: az emberek többsége szívesen segít másokon, különösen, ha valamilyen társadalmi nyomást érez vagy azt látja, a megítélése függ azon, hogy segít-e másokon;
- a reciprocitás elve: ha segít valaki nekünk, a lekötelezettjének érezzük magunkat, és mi is segíteni akarunk neki, hogy ne legyünk az adósai;
- hiszékenység, naivitás, kíváncsiság, befolyásolhatóság;
- monotonitás, figyelmetlenség: minél unalmasabb a munkánk, ingerszegény környezetben, nap, mint nap ugyanazt kell végeznünk, nem fogunk olyan körültekintően eljárni, amely során kiszűrhetjük az esetleges támadásokat;

[6] *Kevin Mitnick napjaink egyik leghíresebb hackere, aki magát sosem tartotta igazán kiemelkedő hackernek, elmondása szerint sikereit inkább social engineerként érte el. Letartóztatását követően szakított a rendszerekbe történő illegális behatolásokkal, biztonsági céget alapított, azóta etikus hackerként tevékenykedik.*

[7] *Kevin D. Mitnick: A legendás hacker- A megtévesztés művészete. Perfact-Pro, Budapest, 2003.*

[8] *Deák Veronika: A social engineering humán alapú támadási technikái, In. Biztonságpolitika, 2017. április 10., http://biztonsagpolitika.hu/publikaciok-2017/deak-veronika-a-social-engineering-human-alapu-tamadasi-technikai*

[9] *Oroszi Eszter Diána: Social engineering- Az emberi erőforrás, mint az információbiztonság kritikus tényezője, Budapesti Corvinus Egyetem Gazdálkodástudományi Kar, 2008., http://krasznay.hu/presentation/diploma_oroszi.pdf*

[10] *I.m. Deák 2017.*

- szexualitás: nem csak a szex, de annak az ígérete is sok esetben feledteti a biztonságtudatosságot, és veszi rá a célszemélyt olyan dolgok elvégzésére, amit egyébként nem tenne meg.

Tovább bonyolítja a kérdést, hogy igen széles skálán mozog az emberek adatvédelmi és információbiztonsági tudatossága. Ide tartozik még a digitális szakadék, ami emberek csoportját választja el az infokommunikációs technológiák szempontjából. A szegregált információs társadalomban szakadék képződik a digitális írástudatlanok és az írástudók között. Az előbbiek nem élvezhetik a technológiai fejlődés nyújtotta előnyöket, miközben tartósan kiszorulnak a gazdaság azon növekvő területeiről, amelyeken az info-kommunikációs eszközök használata olyan alapkövetelménnyé vált, mint a hagyományos írni-olvasni tudás. Nem nehéz belátni, egy digitális írástudatlan munkavállaló, akinek információbiztonsági tudatossága is alacsony, mekkora kockázatot jelent, hiszen vélhetően fel sem ismeri a támadási kísérleteket, amik ellen védekezhet, adott esetben jelezheti egy kompetens személynek, aki elháríthatja. Ezek azok a munkavállalók, akik a social engineerek célpontjává válnak.

Egy rendszerbe történő behatolás a kiépített védelmi szint függvényében változó költségekkel jár. Minél értékesebb információt tárolnak a rendszerben, annál magasabb költségek mellett realizálható az informatikai támadás is, hiszen olyan tudású hackereket kell megvásárolni, akik képesek behatolni a rendszerbe, emellett drága eszközökre is szükség van, ami jelentősen növeli a támadók költségeit. Ebből következően sokszor egyszerűbb social engineering támadást végrehajtani. Ilyenkor a támadók megkeresik azt a gyenge láncszemet a védelemben, akin keresztül elérhetik a céljaikat. Ha az elsődlegesen kinézett célszemély nem jár eredménnyel, mást keresnek, egészen addig, amíg meg nem találják az alkalmas célszemélyt. Minél nagyobb egy munkahely, annál nagyobb az esély, hogy megtalálják azt az egy személyt, akin keresztül megtámadhatják a rendszert. A 2010-ben felfedezett Stuxnet vírus, ami egyes vélemények szerint hat évvel vetette vissza az iráni nukleáris programot, a legenda[11] szerint egy fertőzött pendrive-on jutott be a natanzi létesítménybe.[12] Mint ez az eset is alátámasztja, a social engineering-nek igen komoly hatása is lehet, hiszen rajta keresztül nem csak információkat lehet szerezni, hanem kritikus infrastruktúrák támadására is alkalmas, ráadásul olyan célpontok ellen is sikeresen alkalmazták már, mint egy urándúsító üzem.

A social engineering támadásokat célszerű megkülönböztetni az alapján, hogy informatikai eszközökkel (IT alapú) vagy anélkül (humán alapú) követik el.

[11] *Legenda alatt a fedőtörténetet értem*

[12] *Gyebrovszki Tamás: Stuxnet - mint az első alkalmazott kiberfegyver - a Tallinni Kézikönyv szabályrendszere szempontjából, In. Hadmérnök, IX. évolyam, 1. szám, 2014. március, pp. 164.174.*

Humán alapú támadások széles körét különböztethetjük meg.[13] Közös pont esetükben, hogy nem a technológia sérülékenységét használják ki, hanem a korábban említett emberi tulajdonságokat. Az ilyen jellegű támadások speciális képességeket igényelnek a támadóktól, hiszen szemtől szemben kell végrehajtani, így képes kell legyen az általa választott legendát a lehető leghihetőbben eljátszani, miközben magas szintű érzelmi intelligenciával is rendelkeznie kell.

A humán alapú támadások közé soroljuk az alábbiakat:

- segítségkérés: sok esetben sikerrel járnak a támadók, ha valamilyen információt kérnek. Ez természetesen csak egy lépése a végcélnak, de sokszor nagyon jó alapot ad a további információgyűjtésnek, pl. egy munkatársról olyan elsőre érdektelennek tűnő információk, amik a támadónak hasznosak lehetnek a későbbiekben. Elsődleges célpontjai a help deskek, titkárságok, ügyfélszolgálatok, recepciók munkatársai;
- segítség nyújtása (fordított social engineering): a támadó első lépésként valamilyen problémát okoz, aminek segédkezik a megoldásában, ezzel kiépítve a bizalmat a célpont és közte, majd ezt használja ki a továbbiakban, például előzetesen egy olyan kártevőt küld az áldozat számítógépére, ami akkor fejti ki hatását, amikor a támadó is jelen van;
- identitás lopás: a támadó a számára legelőnyösebb álcát ölti magára, az alkalmazottak, különösen nagyobb munkahelyeken nem ismernek mindenkit, így könnyebben vezethetik meg a gyanútlan munkatársakat. Ilyenkor szervezeten belüli (például karbantartónak, rendszergazdának, más szervezeti egység vezetőjének, új munkatársnak) vagy szervezeten kívüli (például futárnak, valamilyen fontos embernek, hivatalos személynek, auditornak) személyek álcáját veheti fel;
- sírkő lopás (thombstone theft): ritka, de létező támadási forma, a támadó azt használja ki, hogy a vállalatok informatikai rendszerét nem frissítették, és olyan személyek jogosultságait is tartalmazza még a rendszer,[14] akik már nem dolgoznak a munkahelyen;
- felhatalmazás: a támadó egy harmadik félre hivatkozva kér valamilyen információt- például egy szabadságon levő munkatárs kérte meg, hogy

[13] *I.m. Deák 2017.*

[14] *Általában ennek oka az integritás hiányában található meg, például az informatikusok vagy a HR-esek nem kommunikálnak egymással, a HR-esek nem jelzik az informatikusoknak, hogy kik nem dolgoznak már a szervezetnél, így ennek az információnak a hiányában az informatikusok nem törlik a rendszerből az érintett személyeket. Előfordulhat az is, hogy más munkakörbe kerül egy alkalmazott, ami nem követel meg olyan szintű hozzáférést, mint ami az előző munkakörében volt, de ez az információ sem jut el az informatikusokhoz, így továbbra is azzal a hozzáférési szinttel rendelkezik a munkatárs.*

határidőre készítsen el egy jelentést, amihez nincs meg minden információja, így ahhoz kér adatokat;

- jelszavak kitalálása: sok esetben nem szükséges a jelszavakat valamilyen algoritmus használatával feltörni, gyakran kitalálható a felhasználó jelszava, mert nem megfelelő jelszó szabályt alkalmaznak. Még mindig rendkívül gyakori az „12345678", „abdc1234" „jelszó" és egyéb ezekhez hasonló jelszó. Ennél valamivel bonyolultabb, de ugyanúgy könnyen kitalálható jelszó a felhasználóra utaló szavak, születési ideje, kutyája neve stb. A segítségkérés esetében megszerzett információk adott esetben is hasznosak lehetnek, például a célszemély e-mail címe, ami egy gyakori vezetéknév esetén sokszor a születési idejét is tartalmazza;
- baráti üdvözlet: ismeretlenekkel szemben, ha bizalmatlanok is vagyunk, a barátaink esetében már nem vagyunk ennyire óvatosak. A támadók ilyenkor barátaink nevében küldenek például valamilyen fertőzött filet, amit bízva a küldő személyben, megnyitunk;
- Bejutás az épületbe: számos módja van a technikának, sokszor ez is megkövetel valamilyen álcát, pl. takarítóbrigádhoz csatlakozunk, cigiszünetet tartó munkatársakhoz stb. Használhatnak hamis belépőkártyát, ami lehet egy sima fehér lap, amire rányomtatták a támadó fényképét, a szervezet logóját, és belépéskor fontos embernek adja ki magát a támadó, miközben valami fontos emberrel telefonál, bízva abban, hogy elég csak felmutatnia a kártyát, az őrök nem ellenőrzik rendesen, és beengedik anélkül, hogy a kártyát le kellene húznia az érintőpanelen;
- más jogosultságának felhasználása (piggybacking): a támadó egy szervezeten belüli munkatársnak adja ki magát, aki otthon felejtette a belépőkártyáját, kulcsait stb.;
- kukabúvárkodás (dumpster diving): mindig célszerű átvizsgálni a célszemély szemetesét, hiszen rengeteg értékes információhoz férhetünk így hozzá. Ez mind szervezetek, mind magánszemélyek esetében hasznos lehet;
- váll szörfölés (shoulder surfing): a támadó úgy helyezkedik el a célszemély körül, hogy kileshesse jelszavát, pin kódját.

Az IT alapú támadások esetén a támadó valamilyen informatikai eszköz segítségével téveszti meg áldozatát.[15] A humán alapú támadásokkal ellentétben nem informatikai jellegű kompetenciákat követel meg a támadótól.
Az IT alapú támadások a következők:

- adathalászat (phishing): a támadásnak több vállfaját különböztetjük meg:

[15] *Deák Veronika: A számítógép alapú social engineer támadási technikák, In. Biztonságpolitikai, 2017. április 28., http://biztonsagpolitika.hu/publikaciok-2017/deak-veronika-a-szamitogep-alapu-social-engineering-tamadasi-technikai*

- hamis e-mailek és weboldalak: ezek a támadások szofisztikáltságuktól függően nagyon eltérőek. A támadók olyan weboldalakat hoznak létre, ami külsőségeiben hasonlít egy létező oldalra (gyakran pl. banki oldalakra), és ezeket vagy e-mailben vagy nem túl megbízható weboldalaknál teszik közzé felugró ablakként. A többségére jellemző, hogy valamilyen internetes fordítóprogram segítségével fordították le a szöveget, ami így magyartalan mondatokat eredményez, de ennek ellenére így is nagy számban sikerül megtéveszteni embereket. Pénzügyi tranzakciókat másoló oldalak esetében többségében az adathalász oldalak nem titkosított kommunikációt biztosító kapcsolaton üzemelnek,[16] amit egy tudatos internetező egyből kiszúr;
- vishing: hang alapú adathalászat, alapvetően valamilyen VoIP[17] technológiát használó támadás;
- smishing: sms-ben történő támadás;
- pharming: eltérítéses adathalászat, amikor a támadók nem szimplán létrehozzák a másolatát egy weboldalnak, hanem a szolgáltatás domain nevének eltérítésével irányítják a hamisított weboldalra. Ez esetben hiába írja be a felhasználó az URL-t, amit fel szeretne keresni, a támadók ezt az elérési útvonalat támadják meg, a DNS-szerver egy másik IP címre irányítja a felhasználót. Ha a támadók valósághűen másolják le az eredeti oldalt, ráadásul ügyelnek arra is, hogy az oldal titkosított kapcsolaton keresztül üzemeljen, nagyon nehéz dolga van a felhasználónak, hogy kiszűrje; [18]
- whaleing: az adathalászat egy specifikusabb verziója, ebben az esetben vezetők a célpontok, gyakran több lépcsős támadást építenek fel, hogy sikerrel járjanak.

---

[16] A kapcsolat csak HTTP és nem HTTPS- az S jelzi a titkosított kapcsolatot. Titkosított kapcsolat esetén általában a böngészők címsorában egy zöld lakat is szerepel, de a böngészők gyakran e mellett „biztonságos" felirattal jelzik.

[17] Internetprotokoll feletti hangátvitel, olyan telekommunikációs forma, ahol a kommunikáció nem hagyományos telefonhálózaton keresztül valósul meg, hanem IP-alapú adathálózaton.

[18] Hasonló módon, egy egész bankot „loptak el" támadók Brazíliában. A támadás során a bank weboldalait, kártyaleolvasóit, ATM automatáit ilyen módon a saját hamisított weboldalukra irányították. Bővebben lásd: Hanula Zsolt: Hekkerek egy egész bankot elloptak Brazíliában, In. Index, 2017. április 6., https://index.hu/tech/2017/04/06/hekkerek_egy_egesz_bankot_elloptak_braziliaban/ (Letöltés dátuma: 2017. december 28.)

- kártékony programok: a támadás során olyan rosszindulatú kódok vannak elrejtve az eszközön vagy a file-on, amelynek segítségével szerezhetik meg a célszemély adatait. Ennek módja lehet:
    - frissítés, javítás felajánlása: a támadók sokszor olyan tartalommal környékezik meg a célszemélyt, amelyben egy biztonsági frissítés vagy adott esetben egy vírusfertőzésre való figyelemfelkeltés, és az általuk javasolt frissítés, vírusirtó megmenti a felhasználót a káresemény bekövetkezésétől. Az informatikában kevésbé járatos felhasználók egy ilyen üzenettől általában megriadnak, és telepítik a felajánlott programot. Különösen gyakori ez a támadástípus az okos mobil eszközök esetében.
    - billentyűzet-naplózó (keylogger): a támadás lényege, hogy a megfertőzött eszközön a kártevő minden leütött billentyűt megjegyez, és az erről készített naplófileokat elküldi a támadók részére;
    - trójai programok: a trójai programok a kártevőknek azon változatai, amelyek segítségével a támadók egy hátsó kaput nyitnak az áldozat eszközén, és így szereznek hozzáférés az azon szereplő adatokhoz. Gyakran olyan programokba ágyazzák, amelyek valóban valami hasznos tevékenységre valóak;
    - veszélyes csatolmányok: a támadók olyan e-mailt küldenek, amelyben a csatolmány valamilyen kártékony kódot tartalmaz. Ennek fejlettebb módszere, amikor mindezt pl. egy barátunk nevében teszik.
- baiting: a támadás során különböző adathordozókat (DVD, pendrive eszközöket19 stb.) szórnak szét a támadók, amelyek kártékony kódokat tartalmaznak, majd a számítógéphez való csatlakoztatást követően fertőzi meg az eszközt. Ilyenkor szándékosan figyelemfelkeltő tartalmakat „ígérnek”, pl. a DVD-k „blockbuster” filmeket, erotikus tartalmakat tar-

[19] *A 2017. évi XXXIII. OTDK Had- és Rendészettudományi Szekciójának Kiberbiztonsági Tagozatában első helyezést ér el Deák Veronika dolgozata, amely egy hasonló kísérletet végzett el. A kísérletben egy „mobiltöltő” feliratú dobozt helyezett el a Nemzeti Közszolgálati Egyetem egyik Karán, és azt vizsgálta, hányan csatlakoztatják az ismeretlen eszközre a telefonjukat. Ez azt a kockázatot rejti magában, hogy az adatkábel segítségével megfertőzhetik kártékony programokkal a csatlakoztatott készüléket. A témáról bővebben lásd: Deák Veronika: Biztonságtudatosság az információs környezetben, In. Szakmai Szemle- A Katonai Nemzetbiztonsági Szolgálat Tudományos- Szakmai Folyóirata, 2017/3., pp. 59-77., 2017.*

talmaznak a felírás szerint, így véve rá a célszemélyt, hogy lejátssza. Célzott támadás esetén humán alapú technikákkal is vegyíthetik.[20]

- Wi-Fi hálózat veszélyei: a hálózat üzemeltetője képes monitorozni a hálózaton zajló adatforgalmat. Napjainkra talán kezd tudatosulni, hogy egy nyílt Wi-Fi hálózat milyen kockázatokkal jár, azonban sajnos gyakran nincsenek tisztában azzal, hogy a jelszóval védett hálózatok ugyanúgy lehetnek veszélyesek, ugyanúgy megfigyelhetnek azon keresztül a támadók. Igaz ez a biztonságosnak hitt otthoni hálózatunkra is. A felhasználók döntő többsége a router jelszavát alapértelmezetten hagyja, ami egy egyszerű Google-os kereséssel (ha ismerjük a router típusát) kikereshető.
- alkalmazásengedélyekből fakadó kockázatok: az okos mobil eszközökre telepített alkalmazások a használatért cserébe különböző engedélyeket kérnek. Ezek az engedélyek sok mindenre vonatkozhatnak: üzeneteink tartalmához, ismerőseinkhez, megosztott tartalmaink, geolokációs helymeghatározáshoz, kamera és mikrofon vezérléséhez, az eszközön tárolt fileokhoz. A felhasználók nagy része egyáltalán nem olvassa el egy alkalmazás telepítése során, hogy mihez ad engedélyt, éppen ezért rengeteg alkalmazást adathalász célból készítenek el.

A social engineering támadás négy lépésből épül fel. Az első fázis az információgyűjtés. Ennek során választják ki a támadók a „leggyengébb láncszemet" a szervezetnél, akin keresztül hozzáférnek majd a kívánt rendszerhez. Ha megvan a célszemély, a lehető legtöbb információt igyekeznek összegyűjteni róla, hiszen mindez kulcsfontosságú egy olyan legenda kiépítéséhez, amivel akár a bizalmába tudnak férkőzni, akár zsarolással próbálják rávenni az áldozatot a céljaik segítésére. Az információgyűjtés történhet online és „offline" egyaránt. Utóbbira álljon itt egy rövid esettanulmány: egy jövőbeni tanulmányunk témája egy kérdőíves kutatás, amelyben egy klasszikus social engineering támadást szimuláltunk 2017 májusában, a Ludovika Fesztiválon. A kísérlet során egy nyereményjátékot hirdettünk, pár ezer Ft-ot érő pendriveokat nyerhettek a kérdőívünk kitöltői. A kérdőív a kitöltő biztonságtudatosságára vonatkozott, néhány egyszerű kérdést tartalmazott mindössze, illetve utána különböző személyes adatokat kérdeztünk „statisztikai célból".[21] A kérdések többek között a kitöltő munkahelyére, beosz-

[20] Például, kormányablakban a támadó ott felejti a pendriveot, miközben úgy viselkedik, hogy a következő kapcsolatfelvételnél a célszemély mindenképpen emlékezzen rá. Később felhívja kétségbeesetten, hogy nem találja sehol a pendrivejét, de rajta van a gyerekének a határidős feladata, amit ki akart nyomtatni. Sajnos nem tud bemenni, mert dolgozik, de ha átküldené e-mailben a rajta található filet, megmentené a gyereket a bukástól.

[21] Természetesen, hogy ne sértsünk jogszabályt, a megadott válaszokat ezt követően a kitöltőnek visszaszolgáltattuk, semmilyen formában nem kezeltük a személyes adatokat.

tására, e-mail címére, személyi igazolvány számára, születési idejére, kapcsolati státuszára, láb- és ruhaméretére vonatkoztak. A kérdőív tartalmazott egy adatkezelési nyilatkozatot 7-es betűmérettel megfogalmazva, amelyen többek között 3000 évre az Nemzeti Közszolgálati Egyetem Kiberbiztonsági Akadémiájára ruházta a lelkét, továbbá vállalta évi 16 tonna szén előállítását. Erősítendő a bizalmat, minden segítőnknek egy babakék színű passz lógott a nyakában, amelyen az Egyetem logója rendkívül rossz minőségben, szétnyújtva szerepelt, szervezetként „NKE Kiberbisztonsági Akadémija" (sic!), valamint olyan fantázianeveket tartalmazott, mint például „Ipsz Ilonka", „Zsíros B. Ödön". A kísérlet során vizsgáltuk azt is, hányan szúrják ki az adatkezelési nyilatkozatot, illetve a passzt. A válaszadók több mint 90%-a gondolkodás nélkül megadta minden személyes adatát, hiába furcsállották, miért van szükség lábméretre, kapcsolati státuszra, személyi igazolvány számra, a „statisztikai célból" gyűjtjük választ követően megadták. 108 kitöltőből egy sem szúrta ki, hogy a nyakunkban lógó passz miket tartalmaz, valamint 10 alatt volt azoknak a száma, akik elolvasták az adatkezelési nyilatkozatot. A kísérlet során feltételeztük, hogy a Ludovika Fesztiválon magasabb lesz a biztonságtudatossága azoknak, akik az Egyetemmel vannak valamilyen kapcsolatban, sajnos ezt a kísérlet finoman szólva sem támasztotta alá.

A következő lépés a kapcsolat kiépítése, amelynek során az előzetesen gyűjtött információkat felhasználva a célszemély bizalmába férkőznek. Gyakran cél ilyenkor a bizalom erősítése, hogy a későbbiekben hatékonyabban manipulálhassák a célszemélyt. Harmadik fázis a kapcsolat kihasználása, végezetül pedig a támadás végrehajtása az utolsó pont.

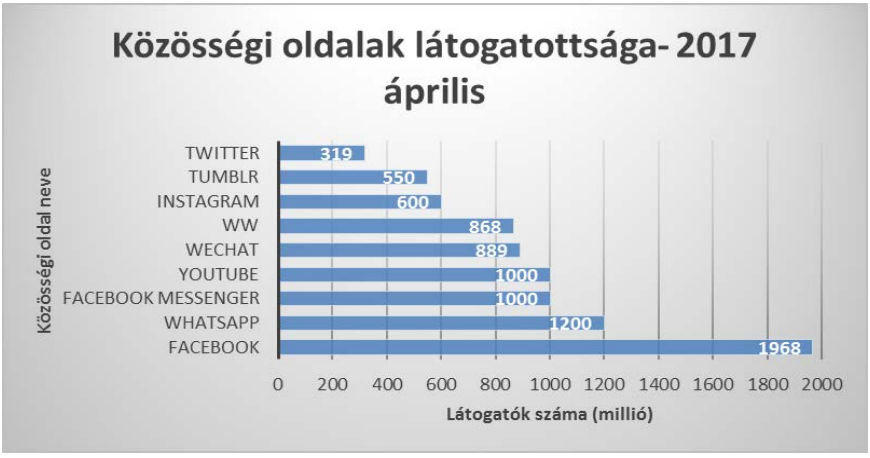
Social engineering a közösségi médiában

A tanulmány elején említett munkámban részletesen bemutattam a közösségi oldalak statisztikai adatait, ez esetben csupán egy adatra hívnám fel a figyelmet (1. számú ábra). A Facebook, mint legismertebb közösségi oldal, az aktív felhasználók naponta közel 2 milliárd embert jelentenek. Ez a fajta használat véleményem szerint determinálja, hogy a támadók éljenek ezen oldalak nyújtotta lehetőségekkel, már csak azért is, mert mint látni fogjuk, nem csupán az információgyűjtésben lehet szerepük, hanem különböző támadástípusokat is végrehajthatnak.

Szükséges röviden a közösségi média fogalmát is tisztáznom. Egy korábbi, szintén a Nemzetbiztonsági Szemlében publikált tanulmányomban[22] ezt részletesen elvégeztem, de az általam alkalmazott fogalmi meghatározás indokolttá teszi, hogy érintőlegesen itt is foglalkozzak a kérdéssel. Értelmezésemben a közösségi média internetes alkalmazások és oldalak összessége, amelyben a szol-

[22] *Bányász Péter: A közösségi média, mint a nyílt forrású információszerzés fontos területe, In. Nemzetbiztonsági Szemle (Online) 2015., III:(2) pp. 21-36.*

gáltató csupán egy keretet biztosít, a tartalmat a felhasználó állítja elő. A kulcsszó ez esetben az alkalmazás, ugyanis ez kibővíti a közösségi média körét az okos mobil eszközök egy jelentős részével, hiszen számos alkalmazás egyrészt integratív szerepet tölt be (más típusú biztonsági kockázatai vannak például a Facebook mobilos verziójának, mint a hagyományosnak), másrészt az alkalmazások gyakran csupán a keretet biztosítják. A tartalomgyártás a felhasználókon múlik (például a különböző VoIP alapú üzenetküldő alkalmazások, amelyek fórumként is működnek, pl. Telegram Messenger).



4. ábra Közösségi oldalak látogatottsága 2017. áprilisában
(saját szerkesztés, Forrás: Statista.com)

Ahogy az előző fejezetben a támadás felépítésénél megfogalmaztam, az első lépés az információgyűjtés. A közösségi média ebben a tekintetben különösen hasznos eszköz,[23] hiszen az átlag felhasználók biztonságtudatossága nem nevezhető túlságosan magasnak. Ráadásul minél hosszabb ideje használunk valamilyen közösségi oldalt, annál több információ gyűjthető össze rólunk, különösen akkor, ha nem figyelünk az adatvédelmi beállításainkra, és nem korlátozzuk, hogy kik férhetnek hozzá az általunk megosztott tartalomhoz. A legnagyobb gond, hogy ezeknek a nyílt forrású információknak a megszerzése rendkívül gyorsan történik. Nem szükséges ehhez magas szintű informatikai képzettség, bizonyos legálisan használható weboldalakon pár perc leforgása alatt összegyűjthetjük azokat a nyílt forrásból megszerezhető információkat, amelyeket a felhasználó megosz-

[23] *Uo.*

tott magáról.[24] Természetesen nem csupán nyílt információkat gyűjthetnek a támadók a célszemélyek közösségi oldalaikról, ám azok már illegális tevékenységnek minősülnek. Ilyen célzott támadás elkövetéséhez is különböző eljárásokat alkalmazhatnak, de mindegyik esetében a cél azonos: hozzáférést szerezni a célszemély adataihoz. Történhet ez:

- a célszemély közösségi oldalának feltörésével. Ez esetben sem feltétel magas szintű informatikai képzettség, a Darkneten megvásárolhatóak olyan tool-ok, amelyek helyettünk végzik el ezt a tevékenységet;
- hamis profilok létrehozásával, amelyek segítségével felveszik a kapcsolatot a célszeméllyel. A támadók azt használják ki, hogy gyakran ismeretlen embereket is visszajelölnek a felhasználók. Természetesen ehhez igyekeznek olyan profilt készíteni, amelyet nagyobb eséllyel jelöl vissza a célszemély. Ehhez már végezhetnek előzetesen információgyűjtést a célszemély preferenciáiról. Gyakori az az eljárás is, hogy a célszemély egy ismerősének a profilját lopják el, a frissen létrehozott profilt az ismerős nevében regisztrálják, amihez feltöltik az ismerős fényképeit is, majd a bejelöléskor egy üzenetben tájékoztatják a célszemélyt, hogy „hackerek feltörték a profilját/elfelejtette a jelszavát/letiltották", ezért regisztrált újból;
- játékok, kvízek, Facebookos alkalmazások létrehozásával, amelyek a használatáért cserébe hozzáférést engednek a felhasználóknak a profiljuk különböző adataihoz. Legendás e témában egy magyar ékszer webshop, ami egy egyszerű kvízjáték segítségével néhány nap alatt 800 ezer felhasználó adatait szerezte meg. Ők csupán marketing célból használták a „Mi az indián neved?" alkalmazásukat. Számos olyan kvíz örvend nagy népszerűségnek Facebookon, amelyeket egy bizonyos kör készít különböző nyelveken, és a kitöltőknek néhány játékos személyiség tesztre kell felelniük. Minél több ilyen tesztet tölt ki egy felhasználó, annál pontosabb személyiségkép rajzolható meg, határozható meg a preferenciája az egyénnek. A gyakorlatban azok, aki kitöltöttek egy-egy ilyen kvízt, hajlamosak rendszeresen megosztani ilyen tartalmakat. Az így összegyűjtött adatokat gyakran adják el harmadik fél részére marketing célokra. A Cambridge Analytica nevű big data elemző cég az adatbázisának egy részét ilyen formában építette ki, amelyet aztán többek között a BREXIT kampányban a kilépés mellett kampányolók, valamint a 2016-os amerikai elnökválasztási kampányban Donald Trump kampányában használtak nagy sikerrel, hogy olyan célzott politikai hirdeté-

[24] Az oldalak tömeges keresésre is alkalmasak bizonyos variánsok megfogalmazásával, amennyiben a felhasználók adatlapján azok nyilvános információként szerepelnek. Ilyen variáns lehet kor, nem, lakhely, végzettség, munkahely, kapcsolati állapot stb.

seket jelenítsenek meg a célszemély részére, amelyek teljes mértékben egyénre szabottak voltak;[25]

- közösségi oldalakon folytatott kártékony kód kampányok segítségével. A közösségi oldalakon, különösen a Facebookon rengeteg rosszindulatú alkalmazás terjed videóknak, híreknek álcázva privát üzenetekben, a hírfolyamban. Az ilyen módon megfertőzött eszközöket a támadók céljaikra használhatják a továbbiakban;
- okos mobil eszközre megírt adathalász alkalmazások használatával. Számos mobil alkalmazás létezik, amelyek a használatért cserébe indokolatlan engedélyeket is kérnek. Az egyik legismertebb eset a Brightest Flashlight Free nevet viselő androidos alkalmazás, amely 100 millió felhasználóról gyűjtött adatokat és adta el harmadik fél részére. Egy zseblámpa alkalmazás használatához alapesetben a vakuhoz való hozzáférés engedélyezése indokolt, minden egyéb engedélykérés mögött adathalászat valószínűsíthető. Nevezett alkalmazás a vakun felül többek között geolokációs helymeghatározáshoz, felhasználói azonosításhoz is engedélyt kért. Nem nehéz belátni, ha egy alkalmazás a telefon kamerájához, mikrofonhoz, üzeneteink tartalmához is engedélyt kér, mi pedig gondatlanul megadjuk, milyen mértékben engedünk hozzáférést a tökéletes megfigyelésünkhöz;[26]
- adathalász oldalak használatával. Az alacsony szintű információbiztonsági tudatosság jellemzője, hogy a felhasználó ugyanazt a jelszót, e-mail címet használja a különböző fiókjai esetében. Amennyiben egy támadók hozzáférnek egy ilyen profilhoz, nagy valószínűséggel más profiljai esetében is ugyan ezeket a belépési adatokat használja;
- rosszindulatú alkalmazások egyéb úton történő fertőzésével, például csatolmányba ágyazott kártékony kód segítségével;
- Wi-Fi hálózat feltörésével és lehallgatásával.

A felsorolt eljárásokat természetesen ötvözni is lehet.

Képzeljünk el egy olyan szituációt, amelyben a támadók egy sok munkavállalót alkalmazó szervezet informatikai rendszeréhez akarnak hozzáférni. A szervezet az általa kezelt adatok folytán magas szintű fizikai és logikai védelmet épített ki. A támadók social engineering támadást kívánnak végezni. Nyílt forrásból feltérképezik a dolgozókat, lefuttatnak első körben egy keresést a fentebb említett oldal segítségével, amely arra vonatkozik, kik dolgoznak az adott szervezetnél. Amennyiben sikerrel járnak, és találnak olyan jelölteket,

[25] *A témáról bővebben lásd: Bányász Péter: A közösségi média, mint az információs hadszíntér speciális tartománya, In. Hadmérnök, KÖFOP Különszám, pp. 108-121., 2017.*

[26] *Adatokat eltulajdonító androidos zseblámpa alkalmazás, In. GovCERT, 2013. december 6., http://tech.cert-hungary.hu/tech-blog/131206/adatokat-eltulajdonito-androidos-zseblampa-alkalmazas (Letöltés dátuma: 2017. december 28.)*

akik vélhetően hasznosak lehetnek számukra, akkor specifikusan folytatják a nyílt forrású információgyűjtést.[27] Fontos látni, nem feltétlenül szükséges a támadóknak, hogy magas beosztásban levő személyt támadjanak, olyan valakire van szükségük, aki hozzáférhet a rendszerhez, de a biztonságtudatossága alacsony szintű.

Egy titkárnő, egy portás, egy takarító ilyen esetekben ugyanúgy értékes célpont lehet. Előbbi, mert sok esetben ugyanazokhoz az információkhoz hozzáfér, mint a főnökei, utóbbiak pedig például észrevétlenül férhetnek hozzá az informatikai rendszerhez, hálózathoz, ez által feltelepíthetnek olyan alkalmazásokat vagy elhelyezhetnek kibertámadáshoz használatos eszközöket a számítógépekben, amelyek segítségével a támadók hozzáférhetnek az informatikai rendszerhez, akár átvéve fölötte az irányítást.[28] Egyértelműen ki kell jelenteni, a biztonságtudatosság mértéke nem beosztás, munkakör függvénye, ahogy ezt „Emily Williams" esete is igazolja.[29] Két biztonsági kutató létrehozta a nem létező Emily Williams Facebook és LinkedIn profilját, amelyben egy fiatal, csinos, MiT-n végzett, egyedülálló Emily munkát keresett, aki egy, a kutatók által hivatalosan meg nem nevezett, kiberbiztonságért felelős amerikai kormányügynökség munkatársaival kezdett kapcsolatépítésbe. A bizalom fokozatos kiépülésével Emily a partnereitől egyre több állásajánlatot kapott az ügynökségnél, többen randevúra hívták, volt, aki laptopot ajándékozott számára. Következő lépésként Emily egy elektronikus képeslapot küldött a partnereinek, amelyben egy trójai program volt elhelyezve. A képeslapot többen a kormányügynökség számítógépein nyitották meg, ily módon a kutatók hozzáférhettek a rendszerben tárolt bizalmas in-

[27] Itt segíthetnek olyan személyiségjegyek, amelyeket a későbbiekben kihasználhatnak. Az emberek nagy része nyíltan oszt meg olyan tartalmakat, amelyek a komplexusaikra utalnak, magányra, szeretetéhségre, az elismerés hiányára stb.

[28] Szemléletes példa az antwerpeni kikötőt ért kibertámadás, amely során a támadók a kikötő informatikai rendszeréhez fértek hozzá oly módon, hogy valakik néhány kibertámadáshoz használatos eszközt rejtettek el a számítógépekben. Az értékes szállítmányok eltérítése mellett kábítószer- és fegyvercsempészetre is használták a későbbiekben a rendszert. Bővebben lásd: Bányász Péter: Az ellátási lánc kiberfenyegetettsége, különös tekintettel a közlekedési alrendszer biztonságára, a szervezett bűnözés hatásai, In. Humánvédelem -békeműveleti és veszélyhelyzet-kezelési eljárások fejlesztése (szerk. Csengeri János, Krajnc Zoltán), Budapest: Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, pp. 643-673., 2016. Letölthető: http://real.mtak.hu/33554/1/tanulmanygyujtemeny%20_ujratervezes_CsJ_KZ_1.5.pdf

[29] Lakhani, Aamir- Muniz, Joseph: Social Media Deception, In. RSA Konferencia Európa 2013, 2013. október 29-31, http://itcafe.hu/dl/cnt/2013-11/102992/hum-w01-social-media-deception.pdf (Letöltés dátuma: 2018. január 10.)

formációkhoz. Az áldozatok között volt a szervezet informatikai biztonságáért felelős vezető is.

Nyílt forrású információgyűjtést követően megkezdődhet a kapcsolat kiépítése. Ismerve a célszemély preferenciáit, a támadók könnyűszerrel alakíthatják úgy, hogy véletlenszerűnek tűnjön a kapcsolatfelvétel. Hogy mit kezdenek a kapcsolattal, az a támadók céljától függ. Idő függvényében egyre közelebb férkőzhetnek a célszemélyhez, a bizalmába férkőzhetnek, kihasználhatják azokat a komplexusait, amelyekről előzetesen tudomást szereztek (például magány), de folytathatják az információgyűjtést róla, hogy adott esetben meg tudják zsarolni, így kényszerítve ki, hogy megtegye számukra azt, amire szükségük van. Visszautalva a felsorolásra, hogyan férhetnek hozzá illegálisan a célszemély nem nyílt adataihoz is: akár egy fertőzött csatolmányt küldve, akár rávéve egy alkalmazás telepítésére, amelyben mindenhez hozzáférést engedélyez. Könnyen találhatnak ezt követően olyat, amivel megzsarolhatják.[30] Az sem elképzelhetetlen, hogy a célszemélyt másokon keresztül akarják rávenni valamire, például a gyereke bizalmába férkőznek egy hamis Facebook profil segítségével, akitől erotikus képeket csalnak ki, majd ezzel állnak az áldozat elé.

A támadás végrehajtása történhet klasszikus IT alapú technikák használatával is. Azok az eljárások, amiket az információgyűjtés kapcsán fogalmaztam meg a kártékony kódok informatikai eszközre telepítésével, nem csupán megfigyelésre alkalmazhatóak, olyan rosszindulatú alkalmazások is felkerülhetnek a számítógépre, amelyeken keresztül a támadók átvehetik a rendszer feletti irányítást.

Ezt követően, hogy a támadók milyen célt szeretnének elérni, az a motivációjuktól függ. Ahogy korábban is megfogalmaztam, az adatok megszerzésétől kezdve akár egy ország kritikus infrastruktúrájának támadásáig bezárólag lehet a social engineering a támadás része.[31]

Összefoglalás

Tanulmányomban a social engineering és a közösségi média kapcsolatának elemzését tűztem célul, hogy ezzel is felhívjam a figyelmet a közösségi média használatából fakadó kockázatokra. A social engineering a kibertámadásoknak egy olyan típusa, amikor a támadók a humán tényezőn keresztül férnek hozzá a védett informatikai rendszerekhez. Védekezni mégis rendkívül nehéz ellene, hiszen a legkevésbé változtatható tényezőt, az emberi személyiséget kellene megvál-

[30] Például megcsalja a párját, amit egy minden hozzáférést megadott telefonos alkalmazással tudnak bizonyítani: üzenetváltások, geolokációs helymeghatározás, kamera és mikrofon távoli vezérlése és a tevékenység rögzítése.

[31] Kovács László, Krasznay Csaba: A digital Mohács: a cyber attack scenario against Hungary, In. Nemzet És Biztonság: Biztonságpolitikai Szemle III:(Spec. Issue Winter) pp. 49-59. (2010)

toztatni. Az informatikai eszközök terjedésével, a közösségi oldalak és az internethasználat nyomán kialakuló függőségünk, a támadók egyre kifinomultabb támadásaival a jövőben egyre aktuálisabb lesz az általam vizsgált kérdés. Az egyik legfontosabb eszközünk a védekezés során az oktatás, amelynek fel kell hívnia a figyelmet azokra a kockázatokra és kihívásokra, amelyek ezen eszközök használatából ered. A social engineering nem csupán egy adott szervezet munkatársait érinti, hanem mindenkit iskolázottságtól, beosztástól és életkortól[32] függetlenül. A tanulmány megírásakor rendkívül nehéz dolgom volt, hiszen számos olyan példát írtam le egy támadás végrehajtásához, amellyel egyúttal ötletet is adhattam. Úgy gondolom azonban, hogy ennek ellenére fontos ezek ismerete, hiszen csak azok ellen tudunk védekezni, amiről tudjuk, kockázatot jelentenek. Tapasztalatom szerint a biztonságtudatosság növelésére vonatkozó oktatás nem lehet hatékony, ha csupán általánosságban fogalmazzuk meg a fenyegetéseket, ugyanis sok esetben a felhasználók nem érzik valósnak a kockázatokat („Én nem vagyok eléggé fontos"), így nem is védekeznek ellene, mert érzik magukat veszélyben. Reményeim szerint e tanulmány segít növelni a biztonságtudatosságot.

Felhasznált irodalom

- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1300050.tv
- Abraham, S., Chengalur-Smith, I.: An overview of social engineering malware: Trends, tactics, and implications, Technology in Society 32(3), pp. 183-196., 2010.
- Adatokat eltulajdonító androidos zseblámpa alkalmazás, In. GovCERT, 2013. december 6., http://tech.cert-hungary.hu/tech-blog/131206/adatokat-eltulajdonito-androidos-zseblampa-alkalmazas (Letöltés dátuma: 2017. december 28.)
- Bányász Péter: A közösségi média, mint az információs hadszíntér speciális tartománya, In. Hadmérnök, KÖFOP Különszám, pp. 108-121., 2017.
- Bányász Péter: A közösségi média, mint a nyílt forrású információszerzés fontos területe, In. Nemzetbiztonsági Szemle (Online) 2015., III:(2) pp. 21-36.

[32] *Különösen a fiatalkorúak esetében szükséges nagy hangsúlyt fektetni a biztonságtudatossági képzésekre. Bővebben lásd: Krasznay Csaba- Varga- Perke Bálint: Ifjúságvédelem a hacker szubkultúrában, In: Ártalmas vagy hasznos internet?, A média hatása a gyermekekre és fiatalokra (szerk. In: Bíró A Zoltán, Gergely Orsolya), Csíkszereda: Státus Kiadó, pp. 179-202., 2013.*

- Bányász Péter: Az ellátási lánc kiberfenyegetettsége, különös tekintettel a közlekedési alrendszer biztonságára, a szervezett bűnözés hatásai, In. Humánvédelem -békeműveleti és veszélyhelyzet-kezelési eljárások fejlesztése (szerk. Csengeri János, Krajnc Zoltán), Budapest: Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, pp. 643-673., 2016. (http://real.mtak.hu/33554/1/tanulmanygyujtemeny%20_ujratervezes_CsJ_KZ_1.5.pdf)
- Bányász Péter: Kiberbűnözés és közösségi média, In. Nemzetbiztonsági Szemle, 2017/4., pp. 55-74., 2017.
- Boshmaf, Y., Muslukhov, I., Beznosov, K., Ripeanu, M.: Design and analysis of a social botnet, Computer Networks 57(2), pp. 556-578., 2013.
- Crawford, A.: Networked governance and the post-regulatory state?: Steering, rowing and anchoring the provision of policing and security, Theoretical Criminology 10(4), pp. 449-479., 2006.
- Deák Veronika: A social engineering humán alapú támadási technikái, In. Biztonságpolitika, 2017. április 10., http://biztonsagpolitika.hu/publikaciok-2017/deak-veronika-a-social-engineering-human-alapu-tamadasi-technikai
- Deák Veronika: A számítógép alapú social engineer támadási technikák, In. Biztonságpolitikai, 2017. április 28., http://biztonsagpolitika.hu/publikaciok-2017/deak-veronika-a-szamitogep-alapu-social-engineering-tamadasi-technikai
- Deák Veronika: Biztonságtudatosság az információs környezetben, In. Szakmai Szemle- A Katonai Nemzetbiztonsági Szolgálat Tudományos-Szakmai Folyóirata, 2017/3., pp. 59-77., 2017.
- Dodge Jr., R.C., Carver, C., Ferguson, A.J.: Phishing for user security awareness, Computers and Security 26(1), pp. 73-80., 2007.
- Garera, S., Provos, N., Chew, M., Rubin, A.D.: A framework for detection and measurement of phishing attacks, WORM'07 - Proceedings of the 2007 ACM Workshop on Recurring Malcode, pp., 1-8, 2007.
- Gyebrovszki Tamás: Stuxnet - mint az első alkalmazott kiberfegyver - a Tallinni Kézikönyv szabályrendszere szempontjából, In. Hadmérnök, IX. évolyam, 1. szám, 2014. március, pp. 164.174.
- Hanula Zsolt: Hekkerek egy egész bankot elloptak Brazíliában, In. Index, 2017. április 6., https://index.hu/tech/2017/04/06/hekkerek_egy_egesz_bankot_elloptak_braziliaban/ (Letöltés dátuma: 2017. december 28.)
- Kevin D. Mitnick: A legendás hacker- A megtévesztés művészete. Perfact-Pro, Budapest, 2003.
- Kovács László, Krasznay Csaba: A digital Mohács: a cyber attack scenario against Hungary, In. Nemzet És Biztonság: Biztonságpolitikai Szemle III:(Spec. Issue Winter) pp. 49-59., 2010.

- Kovács László - Sipos Mariann: A Stuxnet és ami mögötte van: Tények és a cyberháború hajnala, In. Hadmérnök, V. évfolyam, 4. szám, pp. 163-172., 2010.
- Krasznay Csaba - Simon Béla: Kiberbűncselekmények az online kereskedelemben, In. Hadmérnök XII. Évfolyam KÖFOP különszám - 2017.
- Krasznay Csaba - Varga- Perke Bálint: Ifjúságvédelem a hacker szubkultúrában, In: Ártalmas vagy hasznos internet?, A média hatása a gyermekekre és fiatalokra (szerk. In: Bíró A Zoltán, Gergely Orsolya), Csíkszereda: Státus Kiadó, pp. 179-202., 2013.
- Lakhani, Aamir - Muniz, Joseph: Social Media Deception, In. RSA Konferencia Európa 2013, 2013. október 29-31, http://itcafe.hu/dl/cnt/2013-11/102992/hum-w01-social-media-deception.pdf (Letöltés dátuma: 2018. január 10.)
- Martino, A.S., Perramon, X.: Phishing secrets: History, effects, and countermeasures, International Journal of Network Security 11(3), pp. 163-171., 2014.
- Neasbitt, C., Perdisci, R., Li, K., Nelms, T.: ClickMiner: Towards forensic reconstruction of user-browser interactions from network traces, Proceedings of the ACM Conference on Computer and Communications Security pp. 1244-1255., 2014.
- Oroszi Eszter Diána: Social engineering- Az emberi erőforrás, mint az információbiztonság kritikus tényezője, Budapesti Corvinus Egyetem Gazdálkodástudományi Kar, 2008., http://krasznay.hu/presentation/diploma_oroszi.pdf
- Potharaju, R., Newell, A., Nita-Rotaru, C., Zhang, X.: Plagiarizing smartphone applications: Attack strategies and defense techniques, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 7159 LNCS, pp. 106-120., 2012.
- Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F., Downs, J.: Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions, Conference on Human Factors in Computing Systems – Proceedings 1, pp. 373-382., 2010.
- Simon László- Magyar Sándor: A terrorizmus és indirekt hatása a kibertérben, In. Nemzetbiztonsági Szemle, 2017/3., pp. 89-101., 2017.
- Stringhini, G., Kruegel, C., Vigna, G.: Shady paths: Leveraging surfing crowds to detect malicious web pages, Proceedings of the ACM Conference on Computer and Communications Security pp. 133-144., 2013.
- Tamás Szádeczky: Information Security - Strategy, Codification and Awareness. In: András Nemeslaki (Ed.): ICT Driven Public Service Innovation. Comparative Approach Focusing on Hungary. Budapest, 2014. pp. 109-122 ISBN 9786155305894

- Thonnard, O., Bilge, L., O'Gorman, G., Kiernan, S., Lee, M.: Industrial espionage and targeted attacks: Understanding the characteristics of an escalating threat, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 7462 LNCS, pp. 64-85., 2012.
- Vishwanath, A., Herath, T., Chen, R., Wang, J., Rao, H.R. : Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model, Decision Support Systems 51(3), pp. 576-586., 2011.